PERSONNEL SECURITY
TABLE OF CONTENTS
DM 3545-000

U.S. Department of Agriculture
Washington, D.C.

DEPARTMENTAL MANUAL	NUMBER: 3545-000
SUBJECT: Personnel Security	DATE: February 17, 2005 OPI: Office of the Chief Information Officer, Cyber Security

CHAPTER 9
GENERAL INFORMATION

1 PURPOSE

The purpose of this Departmental Manual is to provide guidance to U.S. Department of Agriculture (USDA) agencies and staff offices on the requirement to provide all personnel with periodic Information Technology (IT) security awareness and training.

2 CANCELLATION

This Departmental Manual will be in effect until superseded.

3 REFERENCES

The following Public Laws and Federal guidance are applicable to this manual:

Public Law 93-502, “Freedom of Information Act of 1980”;

Public Law 93-579, “Privacy Act of 1974”;

Public Law 99-474, “Computer Fraud and Abuse Act of 1986”;

E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. 3531 et seq., Title III, Federal Information Security Management Act (FISMA);

Public Law 104-321, “Electronic Freedom of Information Act Amendments of 1996”;

Public Law 100-503, “The Computer Matching and Privacy Protection Act of 1998”;

Homeland Security Presidential Directive/Hspd-7, Subject: Critical Infrastructure Identification, Prioritization, and Protection;

Copyright Act of 1980, U. S. Code, Title 17;

Electronic Communications Privacy Act, 18 U.S.C. 2701;

5 CFR Part 930, “Employees Responsible for the Management or Use of Federal Computer Systems”;

OMB Circular No. A-130, Appendix III, “Security of Federal Automated Information Resources”;

NIST Special Publication 800-12, “An Introduction to Computer Security: The NIST Handbook”;

NIST Special Publication 800-16, “Information Technology Security Training Requirements: A Role- and Performance-Based Model”;

NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program (Draft);

DM 3510-001, Chapter 2, Part 1, Security Standards for Information Technology (IT) Restricted Space; and

Departmental Regulation 3300-1, “Telecommunications and Internet Services and Use”.

4 SCOPE

This manual applies to all USDA agencies, programs, teams, organizations, appointees, employees and other activities.

5 ABBREVIATIONS

AIS	Automated Information System(s)
CIO	Chief Information Officer
CS	Cyber Security
FRA	Federal Records Act
IRM	Information Resources Management
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PA	Privacy Act
PDD	Presidential Decision Directive
PL	Public Law
USDA	United States Department of Agriculture

6 DEFINITIONS AND TERMS

a Adequate Security –Adequate security is security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

b Application – Application is the system, functional area, or problem to which information technology is applied. A program or group of programs designed for end-users that include database programs, word processors, and spreadsheets.

c Assets - Assets are things of value that require protection. The value of an asset may be monetary or non-monetary. In IT Security, assets include data, hardware, software, physical environments, personnel and telecommunication capabilities.

d Awareness – Awareness is a learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of IT security.

e Baseline Security – Baseline security refers to the minimum security controls required for safeguarding an Information Technology (IT) system based on its identified needs for confidentiality, integrity and/or availability protection.

f Countermeasures and Controls – Countermeasures and controls refer to the procedures or techniques used to prevent the occurrence of a security incident, detect when an incident is occurring or has occurred, and provide the capacity to respond to or recover from a security incident. Basically, they are intended to protect the assets and availability of an IT system. (Synonymous with safeguards)

g Education – IT security education focuses on developing the ability and vision to perform complex, multi-disciplinary activities and the skills needed to further the IT security profession. Education activities include research and development to keep pace with changing technologies and threats.

h Grantee – One to whom a grant is made. In USDA, grant agreements are made with individuals, entities, and academic institutions to perform scientific research and other studies as authorized by law.

i Hackers/Crackers – The term "hacker" is used to describe any individual who attempts to compromise the security of an IT system, especially those whose intention is to cause disruption or obtain unauthorized access to data. A "cracker" is any individual who used advanced knowledge of networks or the Internet to compromise network security.

j Individual Accountability/Responsibility – A basic tenant of IT security is that individuals must be accountable for their actions. If this is not followed and enforced, it is not possible to successfully prosecute those who intentionally damage or disrupt systems, or to train those whose actions have unintended adverse effects.

k Information Technology (IT) – IT refers to computing and/or communications hardware and/or software components and related resources that can collect, store, process, maintain, share, transmit or dispose of data. IT components include computers and associated peripheral devices, computer operating systems, utility/support software, and communications hardware and software.

l IT Security - IT Security is a technological discipline concerned with ensuring that IT systems perform as expected and do nothing more; that information is provided adequate protection for confidentiality; that system, data and software integrity is maintained; and that information and system resources are protected against unplanned disruptions of processing that could seriously impact mission accomplishment. (Synonymous with Automated Information System Security, Computer Security, Information Systems Security, and Cyber Security)

m IT Security Literacy – IT Security Literacy is the first solid step of the IT security training level where knowledge is obtained through training that can be directly related to the individual's role in his or her specific organization.

n IT Security Program - A program established, implemented and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored or disseminated in its Information Technology systems. (Synonymous with Automated Information System Security Program, Computer Security Program, Information Systems Security Program, and Cyber Security)

o IT System – A collection of computing and/or communications components and other resources that support one or more functional objectives of an organization.

p Job Function – Job functions are the duties specific to a job title.

q Learning Continuum – A learning continuum is a representation in which the common characteristic of learning is presented as a series of variations from awareness through training to education.

r Ownership – Ownership is the responsibility for the security of an IT system or asset that must be assigned to a single, identifiable entity, and to a single senior official within that entity. This approach minimizes the potential for unauthorized activities, and maximizes the potential that the individual knows and understands the nature of threats and vulnerabilities associated with the use or maintenance of an IT system.

s Risk – Risk is defined as the probability that a particular security threat will exploit system vulnerability, thereby causing harm to an asset.

t Risk Management – Risk Management is the process whereby the threats, vulnerabilities, and potential impacts from security incidents are evaluated against the cost of safeguards implementation. The objective of Risk Management is to ensure that all IT assets are afforded reasonable protection against waste, fraud, abuse, and disruption of operation.

u Roles and Responsibilities – Roles and Responsibilities are the functions performed by someone in a specific situation and obligations to tasks or duties for which that person is accountable.

v Security Training – Security training is the sum of the processes used to impart a body of knowledge associated with IT security to those who use, maintain, develop or manage IT systems.

w Threat – A threat is an activity, agent or situation (deliberate, accidental or natural act) with the potential for causing harm to an automated information system or activity.

x Training – Training is teaching people the knowledge and skills that will enable them to do their job more effectively. Training is the next step beyond awareness and most commonly involves formal instruction on how to perform specific tasks.

y Vulnerability – Vulnerability is a flaw or weakness that may allow harm to occur to an IT system or activity.